

UNITED STATES DISTRICT COURT

for the
District of Arizona

In the Matter of the Search of

12828 N. Mountainside Dr. #101
Fountain Hills, AZ 85268

Case No.

20-3262MB

(Filed Under Seal)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

As further described in Attachment A

located in the District of Arizona, there is now concealed:

As set forth in Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code/Section	Offense Description
18 U.S.C. § 1030(a)(2)(C)	Fraud and Related Activity in Connection with Computers
18 U.S.C § 1030(b), 371	Conspiracy

The application is based on these facts:

See Attachment C, Affidavit of Probable Cause, Incorporated by Reference

☒ Continued on the attached sheet.

☐ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA
M. Bridget Minder

Bridget Minder
 Digitally signed by MARY
 MINDER
 Date: 2020.11.04 12:54:02
 -07'00'

Subscribed and sworn to telephonically:

Date: 11-4-20 @ 1:24 p.m.City and state: Phoenix, Arizona

Kevin Keefe
 Applicant's Signature

Kevin Keefe, Special Agent, FBI
 Printed name and title

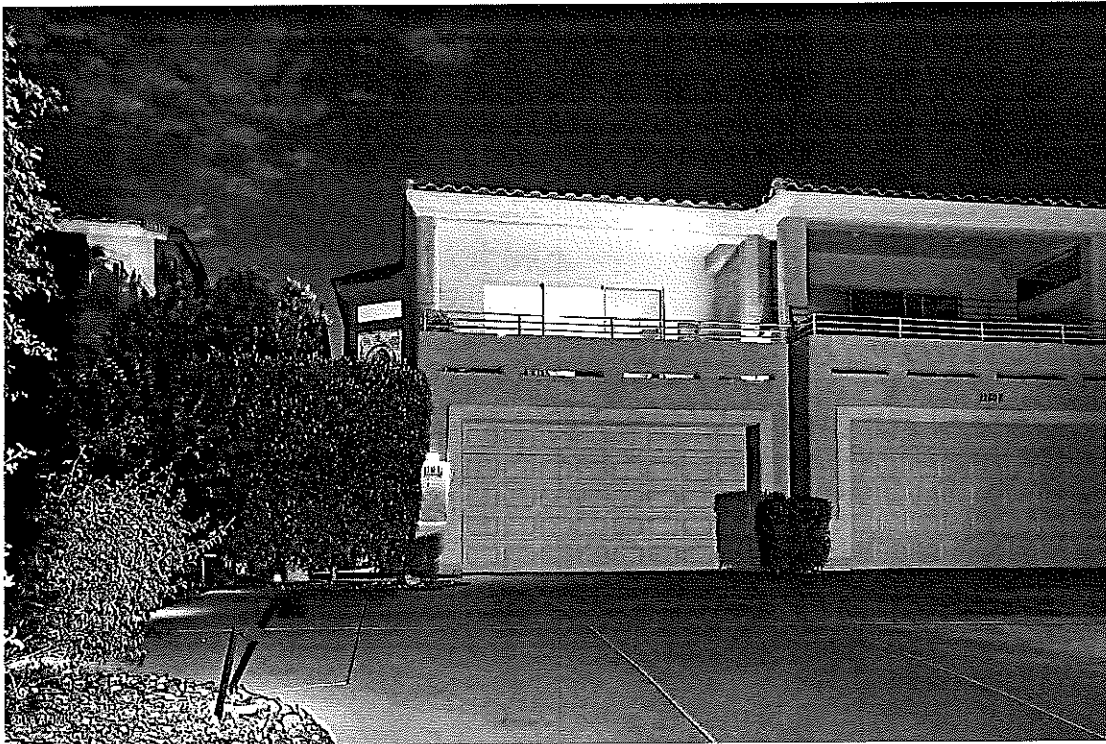
M Morrissey
 Judge's signature

Honorable Michael T. Morrissey, U.S. Magistrate Judge
 Printed name and title

ATTACHMENT A

Property to be searched

The property to be searched is 12828 N. Mountainside Dr., Unit #101, Fountain Hills, AZ, 85268, including vehicles located on the property and the person of Elliot Kerwin (collectively the "PREMISES"). The PREMISES are further described as a two-story townhouse residence, light beige in color and located directly north-west of Mountainside Drive and Andrew Drive, with the numbers "101" posted in large red-brown lettering to the left of the two-car garage, as well as posted to the left of front door.





ATTACHMENT B

Property to be seized

1. The property to be seized at the PREMISES, including in any vehicles located at the PREMISES, is: all computers, tablets or other electronic devices including routers, modems, and network equipment used to connect computers to the Internet (the "SUBJECT DEVICES") which could be used as a means to commit violations of 18 U.S.C. § 1030 (computer intrusion) and 18 U.S.C. § 1030(b) & 371 (conspiracy to commit computer intrusion).

2. The SUBJECT DEVICES will then be searched for records relating to violations of 18 U.S.C. § 1030 (computer intrusion) and 18 U.S.C. § 1030(b) & 371 (conspiracy to commit computer intrusion), which occurred from October 21, 2020 through the present, specifically:

- a. Records, information, and communications relating to any login credentials, accounts, or other access to computer networks of Victim Office;
- b. Records, information, and communications with or relating to Victim Office, including voter registration records and information, including protected voters' information;
- c. Records, information, and communications relating to the transfer, sharing, or dissemination of voter registration records and information, including protected voters' information;
- d. Records, information, and communications relating to the unauthorized access to Victim Office's website and computer systems;
- e. Records, information, and communications relating to attempts or threats to damage or degrade Victim Office's computer systems, including through a denial-of-service attack, malicious software or other means;

- f. Records and information relating to the identity of a botnet;
- g. Records and information related to the identity or location of co-conspirators;
- h. Records and information relating to any e-mail or other communication accounts containing communications related to categories (a)-(g).

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- c. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTER was used;

- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- i. records of or information about Internet Protocol addresses used by the COMPUTER;
- j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- k. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

ATTACHMENT C

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Kevin Keefe, being first duly sworn, hereby depose and state as follows:

1. This application seeks authorization to search for, seize, and forensically search all computers, tablets, and other electronic devices located at 12828 N. Mountainside Drive #101, in Fountain Hills, Arizona. From October 21, 2020 until November 2, 2020, an IP address used at this address gained unauthorized access to voter registration and other personal information of hundreds of thousands of Arizona voters, including hundreds of voters whose information was protected from public disclosure (such as crime victims, judges, and law enforcement personnel). A search of computers, tablets, and other electronic devices found at this location will help law enforcement identify and locate the perpetrator(s) and reveal evidence regarding the means by which the perpetrator(s) gained unauthorized access to the protected information and what the perpetrator(s) did with the confidential and other personal information.

INTRODUCTION AND AGENT BACKGROUND

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 12828 N. Mountainside Drive #101, Fountain Hills, Arizona 85268, including any vehicles on the property and the person of Elliot Kerwin, hereinafter "PREMISES," for computers, tablets, and other electronic devices, as further described in Attachment A, and to search those computers, tablets, and other devices for the things described in Attachment B.

3. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so employed since May 2018. I have received training at the Basic Field Training Course in Quantico, Virginia, with the FBI. My current responsibilities include investigating cyber related

federal crimes to include computer intrusions, phishing campaigns, and ransomware attacks. I have been a federal law enforcement officer since December 2009 and attended the Federal Law Enforcement Training Center in Glynco, Georgia, where I was employed with the United States Marshals Service. Throughout my law enforcement career, I have investigated various crimes to include cybercrimes. During this time, I have participated and executed dozens of search warrants. I am currently assigned to the FBI Field Office in Phoenix, Arizona.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1030(a)(2)(C), Fraud and Related Activity in Connection with Computers, and 18 U.S.C §§ 371 & 1030(b), Conspiracy, have been committed by an unknown subject and other potential unknown subjects. There is also probable cause to search the information described in Attachment A for evidence of these crimes, as described in Attachment B.

PROBABLE CAUSE

6. A county-run government office ("Victim Office") maintains voter registration information for the millions of registered voters who live within the county Victim Office serves. Voter registration information is stored on protected computers, as that term is defined in 18 U.S.C. § 1030(e)(2).¹ Victim Office maintains a website that allows county residents to find their voter

¹ Specifically, Victim Office's computers are protected computers under 18 U.S.C. § 1030(e)(2)(B), which defines protected computers as those used in or affecting interstate commerce, and/or the newly enacted 18 U.S.C. § 1030(e)(2)(C), which defines protected

registration and personalized election information. To access his/her voter registration information and personalized election information, an individual must perform two steps on Victim Office's website:

- a. Enter his/her (i) date of birth, (ii) last name, and (iii) home address number; and
- b. Enter one of the following personal identifiers: (i) last four digits of social security number, (ii) driver's license number, (iii) voter ID number, or (iv) state ID number.

7. Once an individual successfully completed those two steps, he/she could view his/her name, address, voter registration status, ballot status, party affiliation, and permanent early voting list status. If an individual's voter registration and personal information is protected from public disclosure, the website blocks the name, address, voter registration status, party affiliation, and permanent early voting list. Voters who can seek to have their information protected include victims of domestic violence, judges, and law enforcement personnel.

8. On November 2, 2020, Victim Office notified the FBI that it discovered an automated script had been accessing and extracting individual voters' registration information since approximately October 21, 2020 at a rate of approximately 30 voters per minute. (At that rate, it is estimated the script could have accessed registration information for close to 600,000 voters between October 21 and November 2.) Of particular concern, the script also accessed voter registration information, including name and address, for approximately 930 voters whose information is protected from public disclosure.

computers as those that are part of a voting system, that are used for the management, support, or administration of a Federal election, or that have moved in or otherwise affect interstate or foreign commerce.

9. Based on my training and experience, and on information provided by Victim Office, I believe the script exploited the system by which Victim Office formatted the URL for individual voters' registration information.² After an individual completed the steps outlined in paragraph 6 above, the resulting page (displaying the individual's voter registration and personal information) included the voter's seven-digit voter ID number within the URL (An example URL, with the location of the voter ID highlighted, is: /voteridcard/getid.aspx?voterID=XXXXXXX). If the seven-digit voter ID number within the URL was changed, the voter registration information for the individual tied to the new (changed) voter ID would appear. The automated script generated repeated individual requests in the URL, changing the voter ID with each request, to retrieve different voter registration and personal information for hundreds of thousands of registered voters.³ This automated script allowed the perpetrators to evade Victim Office's measures to ensure individuals access only their own information (as described in paragraph 6 above) and to repeatedly access other individuals' voter registration information.⁴

10. According to information provided by Victim Office to the FBI, the unauthorized access of voter registration information between October 21 and November 2 is attributable to a single IP address: 24.56.27.78, which is registered to Cox Communications.

² URL stands for Uniform Resource Locator and is used as a way to identify the location of a file on the Internet.

³ For example, the script would insert at the appropriate place in the URL the voter ID 300001, then it would insert 3000002, then 3000003, and so on.

⁴ Under Arizona law, political parties are provided with voter registration information and voter lists are also available for public inspection at local election offices. Voter information can only be used for non-commercial purposes relating to political party activity, a campaign or election, or for revising election district boundaries. A person in possession of information derived from voter registration forms or precinct registers cannot distribute, post or otherwise provide access to any portion of that information through the internet.

11. Information provided by Cox Communications through legal process revealed that the IP address 24.56.27.78 is leased to the following physical address: 12828 N. Mountainside Dr. #102, Fountain Hills, Arizona. Based on my knowledge and experience, the unauthorized voter registration information was accessed by a computer device attached the IP address located at the mentioned physical address.

12. On November 3, 2020, FBI Special Agents conducted an interview with the homeowner of 12828 N. Mountainside Dr. #102. The homeowner explained to the Agents that she runs the homeowners' association (HOA) for her community and is the account owner for the Cox Internet Service, which is utilized by the HOA and assigned IP address 24.56.27.78. The homeowner shares the internet service registered in her name with a couple (a husband and wife) living in unit #101. The homeowner reported that the husband, Elliot Kerwin, utilizes the majority of the data for the internet service shared by the homeowner in unit #102 and the couple in unit #101.⁵ Between September 11 and October 10, 2020, the homeowner was notified by Cox that the account had used 75% of the billing cycle limit of 1.25 TB (approximately one TB). The homeowner was notified again the following month around October 28, 2020 that the account had reached 75% of the monthly limit, for the billing cycle ending November 10, 2020. The previous average monthly usage was approximately 600 Gigabytes per billing cycle.⁶

13. According to the homeowner in unit #102, Kerwin previously worked for Godaddy.com and currently runs an IT company; his wife works at a propane company. HOA

⁵ According to publicly available records on the Maricopa County Assessor's website, 12828 N. Mountainside Dr. #101 is owned by Elliot and Ellen Kerwin, who purchased the property on October 1, 2018.

⁶ One Terabyte equals a thousand Gigabytes.

rules prohibit home-based businesses, so Kerwin is not to be running any business from his unit. The homeowner also mentioned Kerwin previously owned an IT company called Loon a Tech. Internet research revealed a website, "Loon-A-Tech.com," that lists Kerwin and advertises advanced technology services in computers, laptops, and viruses. The homeowner in unit #102 reported that, approximately one year ago, she received a data usage alert from Cox that she'd reached 75% of the billing cycle limit. When she confronted Kerwin about the alert, he explained the excessive data use was related to his work projects.

14. Based on my training, knowledge, and experience, Kerwin's recent spikes of excessive data usage are atypical for residences and home-based businesses, even in those businesses that provide IT services. Also, based on my knowledge and experience, many home computers come with an overall storage capacity of one TB or less. To put into perspective, open source information shows that in 2009, the Library of Congress contained approximately 74 TB of data.

15. Based on my training, knowledge, and experience, as well as information from Victim Office, the amount of voter registration data accessed that was accessed and extracted between October 21 and November 2 would constitute a large volume of data, consistent with the large volume of data apparently used by Kerwin during this same time period as evidenced by the spike in online data usage activity for the Cox internet service.

16. After Victim Office took measures to stop the unauthorized access and extraction of voter information from its computers originating from IP address 24.56.27.78, FBI received information that, on or around November 3, 2020, the same IP address (24.56.27.78) had conducted activity known as "port scanning" on a website related to a county-run government office in another Arizona county (this second county office's responsibilities also related to voter

registration and conducting elections). Based on my knowledge, training and experience, port scanning is an activity that is frequently performed by criminal actors in an attempt to discover vulnerabilities on a network. Port scanning can be compared to turning the doorknob of a residential door to see if it is unlocked. Computers contain more than 65000 ports, which are communication end points where outside devices can connect. In my knowledge, training, and experience, criminal actors commonly practice port scanning on networks worldwide and exploit vulnerabilities that are found. On the same day, November 3, 2020, the same IP address (24.56.27.78) was also observed attempting to access a voter website in California. The report states that the subject IP address (24.56.27.78) appeared to be reaching out for images on the California county's website. Based on the activity referenced, it is believed that the user of the subject IP address (24.56.27.78) was actively attempting to scan networks for open ports. This is consistent with tactics performed by various criminal actors and enterprises in an effort to collect vulnerabilities, which can be exploited to gain access their network.

17. Based on my training and experience, I know that computers, tablets, and other electronic devices including electronic storage media that are used to commit or contain evidence of computer intrusions are very portable and can be easily stored in vehicles or on one's person. Accordingly, I submit that there is probable cause to search vehicles on the PREMISES as well as the person of Elliot Kerwin for computers, tablets, and other electronic devices that could have been used in the unauthorized access and extraction of voter information from Victim Office's computers.

TECHNICAL TERMS

18. Based on my knowledge, training, and experience, I use the following technical terms in this affidavit to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

19. As described above and in Attachment B, this application seeks permission to search for computers, tablets, and other electronic devices that might be found on the PREMISES. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

20. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered for weeks, months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered weeks, months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users

typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

21. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where,

and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically

also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore,

contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- f. I know that when an individual uses a computer to obtain unauthorized access to a victim computer over the Internet, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

22. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic

picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

23. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

24. Because at least two people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

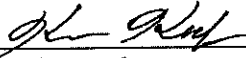
CONCLUSION

25. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

26. This affidavit was sworn telephonically before a United States Magistrate Judge legally authorized to administer an oath for this purpose. I have thoroughly reviewed the affidavit and any attachments, and I attest that there is sufficient evidence to establish probable cause for a search warrant to search the location described in Attachment A for the items described in Attachment B.

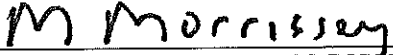
27. In light of the confidential nature of the continuing investigation, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the perpetrators of the unauthorized access and it is possible that there may be other perpetrators who will not be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the various forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,



Kevin Keefe
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to telephonically before me this 4 day of November, 2020



HONORABLE MICHAEL T. MORRISSEY
UNITED STATES MAGISTRATE JUDGE